THE EMBODIMENTS OF THE INVENTION IN WHICH AN EXCLUSIVE PROPERTY OR PRIVILEGE IS CLAIMED ARE DEFINED AS FOLLOWS:

1. A method of masking a conditional jump operation in a cryptographic processor, programmed to execute a sequence of instructions, wherein the conditional jump is determined by evaluating a distinguishing value V against a reference value and wherein the reference value is bounded by an upper limit Vmax and a lower limit Vmin, the method comprising the steps of:
   (a) determining a location of a conditional jump in a program; and
   (b) inserting processor instruction at said location to direct program execution to one of two branches, said processor instructions computing a target address, the target address being derived from said distinguishing value and a base address, wherein for each evaluation of said distinguishing value against said reference value a different number of instructions are executed for each conditional jump.

2. A method as defined in claim 1, said distinguishing value being combined with a random value, thereby adding a random number of instructions on every conditional evaluation.

3. A method as defined in claim 1, said inserted instructions including calls to respective subroutines, said subroutines including instructions for changing the return address of the subroutines to said one of two branches.

4. A method as defined in claim 1, said target address is comprised of said distinguishing value V and a random number.

5. A method as defined in claim 4, said target address is computed using an extended addressing mode of said processor.

6. A method of masking a conditional jump operation in a cryptographic processor programmed to execute a sequence of instructions, wherein the conditional jump chooses one of a plurality of execution branches for execution by comparing a distinguishing value V to a reference value, the method comprising the steps of
(a) associating each of the branches with a respective set of addresses;
(b) computing a target address derived from the value V and said reference value, said target address being located in one of said sets of addresses; and
(c) following the instructions at the target address, said instruction directing program execution to the branch associated with said one of said sets of addresses.

7. A method according to claim 6, wherein each set of addresses contains a plurality of addresses.

8. A method according to claim 6, said instructions at each said target address within a set comprising identical instructions each directing execution to said branch associated with the set.

9. A method according to claim 6, said instructions in a set being sequential operations and random address

10. A method according to claim 6, wherein said instructions at said target address are followed by means of an extended addressing mode of said processor.

11. A method of masking a cryptographic operation using a secret value, comprising the steps of:

(a) dividing said secret value into a plurality of parts;

(b) combining with each part a random value to derive a new part such that the new parts when combined are equivalent to the original secret value; and

(c) utilizing each of the individual parts in said operation.

12. A method as defined in claim 11, including generating a new random value at each use of said secret value.

13. A method as defined in claim 11, said operation being performed in an additive group.

14. A method as defined in claim 11, said operation being performed in a multiplicative group.

15. A method according to claim 11 wherein said new parts are stored after each operation and said new random value is combined with said stored values for use in a subsequent operation.

16. A method according to claim 11 wherein said secret value is used to generate a public key corresponding to the result of a group operation performed with said secret value, said method comprising the steps of performing said group operation on each of said parts to generate a plurality of public keys and utilizing each of said public keys in said operation.

17. A method according to claim 11 wherein said cryptographic operation includes the generation of a signature component utilizing said secret value combined with additional information, said method comprising the step of combining each of said

parts with said additional information and subsequently the results thereof to form said signature component.

18. A method according to claim 17 wherein said results are combined with a further secret value to obtain said signature component.

19. A method according to claim 18 wherein said further secret value is randomly generated for each generation of said signature component.

20. An article of manufacture comprising:

(a) a computer usable medium having computer readable program code embodied therein for masking a cryptographic operation using a secret value, the computer readable program code in said article of manufacture comprising;

(b) computer readable program code configured to cause a computer to divide said secret value into a plurality of parts;

(c) computer readable program code configured to cause a computer to combine with each part a random value to derive a new part such that the new parts when combined are equivalent to the original secret value; and

(d) computer readable program code configured to cause a computer to utilize each of the individual parts in said operation.

21. A method of providing a secret value d for use in a cryptographic operation comprising the steps of

i) selecting a pair of components b_1, b_2 that when combined correspond to said secret value, d,

ii) generating a number π,

iii) combining said number π with respective ones of said components in complimentary manner to generate a pair of updated components such that a combination of said updated components is equivalent to said secret value, d, and storing said updated components.

22. A method according to claim 21 wherein number π is a random number.

23. A method of generating a signature component s for use in a digital signature protocol where s results from an application of a long term private key a, and a short term private key k in a signing process, said method including the steps of representing said long term private key a as a pair of components b_1, b_2, generating a value π, combining said value π with each of said components in a complimentary manner to generate a pair of updated components which, when combined, is equivalent to said long term key, a, performing with said updated components each of the operations normally performed by said long term private key in said signing process, combining the results of said operations to provide a value equivalent to the result of performing said operation with said long term private key, a, and utilizing said value with said private key k to provide the signature component s.

24. A method according to claim 23 wherein said operations include combining said updated components with additional information.

25. A method according to claim 24 wherein said additional information is derived from a message to be signed.